整数のべき乗とオイラーの定理について

青山学院大学　理工学部　物理・数理学科　学籍番号：15111075

中川貴仁　（西山研究室）

2015 年 2 月 20 日

目次

1 序論

今回の論文に書くにあたって、私は先行研究としてフェルマーの小定理を学んだ。この定理を学ぶにつれ、フェルマーの小定理を一般化したオイラーの定理を学ぶことになった。これらの定理は数学において非常に有名なものであるが、私は小林昭七先生の本[1]によってこれを学んだ。

オイラーの定理とは、a と m を互いに素な自然数としたとき、

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

ただし、$\varphi(m)$は、m と互いに素な数の個数である。この関数はオイラーに敬意を表してオイラー関数と呼ばれている。

本論文ではオイラーの定理を用いると法 m の一次方程式を簡単に解くことができることも示した。これは[1]の第 4 章で解説されているが、本論文では少し異なる証明を与えている。

以上は古典的な結果でよく知られているのだが、今回の卒業研究では、a と m が互いに素でない場合についても考え、一体この時に一次合同式がどのような解をもつか、具体的な数字を入れながら確認した。その結果は、下枠内のようになる。

（本文命題１）p,q は相異なる素数とすると $m=pq$ のとき $a^{\varphi(m)}$は 4 種類の数になる。ただし、gcd(a,m)=1, $a \equiv 0 \pmod{m}$ の場合を含む。

これは m の因数が 2 つしかないときであるが、3 つの素因数をもつ場合には以下のようになることがわかっている。

（本文命題２）p,q は相異なる素数とすると $m=pqr$ のとき $a^{\varphi(m)}$は 8 種類の数になる。ただし、gcd(a,m)=1, $a \equiv 0 \pmod{m}$ の場合を含む。

この様な実験的結果から、私は、

m が相異なる n 個の素数の積ならば、$a^{\varphi(m)}$ は法 m で 2^n 種類現れる

という結果を予想し、それを証明することができた。
これこそが、この論文の主定理である（9 ページの定理 4）。

それでは私の論文のはじまりである。どうか最後までお付き合いいただきたい。

2 フェルマーの小定理の一般化 (オイラーの定理)

現代において、インターネットを通じた銀行の取引などには、オイラーの定理を基礎とする RSA 暗号というものが使われている。このオイラーの定理とはいったいどういうものだろうか。この疑問をひも解いていくと、フェルマーの定理というものにさかのぼることが分かった。そこでこの章では、フェルマーの定理とは何か、そしてオイラーの定理とは何かということを見ていこう。

定理 1 (フェルマーの小定理)
p を素数、a を p と互いに素な自然数とすると、$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ。

ここでは、p を素数としたが、これを合成数のときに一般化したのがオイラーの定理である。オイラーの定理を述べるためにまずオイラー関数を導入しよう。

定義 1 m を自然数とする。このとき

$$\varphi(m) = \#\{a \mid 1 \leqq a \leqq m, \gcd(a,m) = 1\}$$

と定義して $\varphi(m)$ を**オイラー関数**という。

定理 2 (オイラーの定理)
mを自然数、a を m と互いに素な自然数とするとき、$a^{\varphi(m)} \equiv 1 \pmod{m}$ が成り立つ。

[注意] m が素数 p のとき、$\varphi(p) = p - 1$ であるから、フェルマーの小定理となる。

証明 1 以上 m 以下の自然数で、m と互いに素なものの個数は定義より$\varphi(m)$である。
これを、

$$r_1, r_2, \ldots, r_{\varphi(m)} \tag{1.1}$$

とする。各 r_i を a 倍して、m でわった余りを r'_i としよう。つまり、

$$ar_i = q_i m + r'_i \quad (0 \leq r'_i < m) \tag{1.2}$$

である。

例えば、$m = 20, a = 3$ のとき、
r は 1, 3, 7, 9, 11, 13, 17, 19 ・・・①
各数を 3 倍して 20 でわると余りは
3, 9, 1, 7, 13, 19, 11, 17 ・・・②
となる。

②は①を並び替えたものであるが、以下一般の $r'_1,\ \dots,\ r'_{\varphi(m)}$ 場合も $r_1,\ \dots,\ r_{\varphi(m)}$を並び替えたものであることを証明する。

まず、$\gcd(r'_i, m) = 1$ である。なぜなら、r'_i とm が共通な素因数q をもつとすると、q は式(1.2)の右辺を割りきるから、左辺 $r'_i a$ もわりきる。よって、r_i か a の少なくとも一方を割りきる。しかし、$\gcd(r_i, m) = 1,\ \gcd(r_i, a) = 1$ より矛盾。よって、$\gcd(r'_i, m) = 1$ である。

もし $r'_i = r'_j$ ならば(1.2)より

$$(r_i - r_j)a = (q_i - q_j)m$$

となり、m は$(r_i - r_j)a$を割りきるが、$\gcd(a, m) = 1$ より、m は$r_i - r_j$を割りきらなければならない。しかし、$1 \le r_i,\ r_j \le m - 1$ より、$|r_i - r_j| < m - 1$ だから、$r_i - r_j = 0$、つまり $r_i = r_j$ である。

以上より、$r'_1, \dots, r'_{\varphi(m)}$ と m は互いに素で、1と m の間にある$\varphi(m)$ 個の整数であることがわかる。したがって、$r_1, \dots, r_{\varphi(m)}$ の順を変えたものである。式(1.2)を

$$ar_i \equiv r'_i \pmod m \qquad i = 1,2, \dots, \varphi(m)$$

と書き直し、これを、$i = 1$ から$\varphi(m)$ まで掛けると

$$(ar_1)(ar_2) \dots (ar_{\varphi(m)}) \equiv r'_1 r'_2 \dots r'_{\varphi(m)} \pmod m$$

となる。 $r'_1, \dots, r'_{\varphi(m)}$ は $r_1, \dots, r_{\varphi(m)}$を並び替えたものだから、

$$a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_1 r_2 \dots r_{\varphi(m)} \pmod m \qquad (1.3)$$

ここで $r_1 r_2 \dots r_{\varphi(m)} = r$ とおくと

$$a^{\varphi(m)} r \equiv r \pmod m$$

$$(a^{\varphi(m)} - 1)r \equiv 0 \pmod m$$

仮定より $\gcd(r_i, m) = 1$ だから $\gcd(r, m) = 1$、したがって $a^{\varphi(m)} - 1 \equiv 0 \pmod m$ であることが証明された。 ■

オイラーの定理を用いると法 m の一次方程式を簡単に解くことができる。

定理 2　　$\gcd(a, m) = 1$ ならば
$ax \equiv b \pmod m$ の解は、$x \equiv ba^{\varphi(m)-1} \pmod m$　で与えられる

証明　$x = ba^{\varphi(m)-1}$ とおくと、

$$ax = a(ba^{\varphi(m)-1}) = a^{\varphi(m)} b \equiv b \pmod m$$

となり確かに方程式の解である。 ■

3 一般の整数のべき乗とオイラーの定理

オイラーの定理において$\gcd(a,m)\neq 1$のときを考えてみよう。
まず、m の因数が 2 つのときを考えてみることにして、$m=pq$ $(p,q$は素数$)$ のときの実験結果を以下に載せる。

・$m=6,\ \varphi(6)=2,\ a^{\varphi(6)}\ (\mathrm{mod}\ 6)$の表

a	2	3	4
$a^{\varphi(6)}$	4	3	4

・$m=10,\ \varphi(10)=4,\ a^{\varphi(10)}\ (\mathrm{mod}\ 10)$の表

a	2	4	5	6	8
$a^{\varphi(10)}$	6	6	5	6	6

・$m=15,\ \varphi(15)=8,\ a^{\varphi(15)}\ (\mathrm{mod}\ 15)$の表

a	3	5	6	9	10	12
$a^{\varphi(15)}$	6	10	6	6	10	6

以上の実験から、$m=pq$ $(p,q$は素数$)$ のとき 2 種類の整数が出てくると予測されるが、それを証明する前に中国式剰余定理について述べる（これについては例えば[2]の第一章を参照してほしい)。

定理 3　$n_1,n_2>0$ を互いに素な整数とするとき、次の(1),(2)が成り立つ

(1) $n_1x_1+n_2x_2=1$ となる $x_1,x_2\in\mathbb{Z}$ をとる. 任意の $a_1,a_2\in\mathbb{Z}$ に対して
$a_0=a_1n_2x_2+a_2n_1x_1$ とおくと、

$$a_0\equiv a_1\ (\mathrm{mod}\ n_1)$$
$$a_0\equiv a_2\ (\mathrm{mod}\ n_2)$$

(2) (1)式を満たすような a_0 は法 n_1n_2 で考えるとただ 1 つしかない。

証明　(1)　$a_0 = a_1(1 - n_1x_1) + a_2n_1x_1 \equiv a_1 \pmod{n_1}$

$= a_1n_2x_2 + a_2(1 - n_2x_2) \equiv a_2 \pmod{n_2}$

となるので、a_0 に対して(1)の 2 式が成り立つ。

(2) a に対しても(1)の 2 式が成り立つなら、

$$a - a_0 \equiv a_1 - a_1 \equiv 0 \pmod{n_1}$$

となる。同様に、$a - a_0 \equiv 0 \pmod{n_2}$ である. よって、$a - a_0$ は n_1, n_2 の公倍数である。n_1, n_2 は互いに素なので、$\mathrm{lcm}(n_1, n_2) = n_1n_2$ である。よって、$a - a_0$ は n_1n_2 の倍数となり、$a \equiv a_0 \pmod{n_1n_2}$ なら、a は(1)の性質を満たす。　■

準備が整ったので、$m = pq$ (p, q は相異なる素数) のとき、整数 a の $\varphi(m)$ 乗は、2 種類の整数になるという証明に移る。

命題 1

$m = pq$のとき、$a^{\varphi(m)}$ は法 mで考えると、4 種類現れる。

[注意]　$\gcd(m, a) = 1$ の時 と $a \equiv 0 \pmod{m}$ の時を含めるので、上で述べたように 2 種類ではなく、4 種類となっている。

証明　$m = pq$ (p, qは素数)として、任意の $a \in \mathbb{N}$ をとると

$$\varphi(m) = pq\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) = (p - 1)(q - 1),$$

$$a^{\varphi(m)} = a^{(p-1)(q-1)}$$

である。まず、$a = sp \quad (1 \le s < q)$の場合を考えると、

$$(sp)^{\varphi(m)} = s^{(p-1)(q-1)}p^{(p-1)(q-1)}$$

であるが、a は p の倍数より p で割った余りは 0 である。 また、$\gcd(s, q) = 1$ および $\gcd(p, q) = 1$ なので、フェルマーの小定理より、$s^{q-1} \equiv 1 \pmod{q}$, $p^{q-1} \equiv 1 \pmod{q}$ となって

$$(sp)^{\varphi(m)} \equiv \begin{cases} 0 & \pmod{p} \\ 1 & \pmod{q} \end{cases}$$

であることがわかる。

次に、$a = tp \quad (1 \leq t < p)$ とすると、p とq の役割を入れ替えることにより、

$$(tq)^{\varphi(m)} \equiv \begin{cases} 1 & (\mathrm{mod}\, p) \\ 0 & (\mathrm{mod}\, q) \end{cases}$$

以上から、中国式剰余定理より、解は法 m で考えると、それぞれ一つに定まる。よって、$\gcd(a,m) \neq 1, m = pq$ のとき、$a^{\varphi(m)}$ は、2 種類の整数である。ゆえに、$\gcd(m,a) = 1$ の時 と $a \equiv 0 \ (\mathrm{mod}\, m)$ の時を含めると、$a^{\varphi(m)}$ は4種類となる。■

次に m の因数が 3 つのときを考えてみることにして、$m = pqr \ (p,q,r$は素数$)$ のときの実験結果を以下に載せる。

・$m = 2 \cdot 3 \cdot 5 = 30,\ \varphi(30) = 8,\ a^{\varphi(30)} \ (\mathrm{mod}\, 30)$の表

a	2	3	4	5	6	8	9	10	12	14
$a^{\varphi(30)}$	16	21	16	25	6	16	21	10	6	16

15	16	18	20	21	22	24	25	26	27	28
15	16	6	10	21	16	6	25	16	21	16

・$m = 2 \cdot 3 \cdot 7 = 42,\ \varphi(42) = 12,\ a^{\varphi(42)} \ (\mathrm{mod}\, 42)$の表

a	2	3	4	6	7	8	9	10	12	14	15	16	18
$a^{\varphi(42)}$	22	15	22	36	7	22	15	22	36	28	15	22	36

20	21	22	24	26	27	28	30	32	33	34	35	36	38	39	40
22	21	22	36	22	15	28	36	22	15	22	7	36	22	15	22

以上の実験から、$m = pqr \ (p,q,r$は素数$)$ のとき 6 種類の整数が出てくると予測される。

命題 2

$m = pqr$のとき、$a^{\varphi(m)}$ は法 mで考えると、8 種類現れる。

[注意]　$\gcd(m,a) = 1$ の時と $a \equiv 0 \ (\mathrm{mod}\, m)$ の時を含める。

証明　$m = pqr$ $(p, q, r$は素数)として、任意の $a \in \mathbb{N}$ をとると

$$\varphi(m) = pqr\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right) = (p-1)(q-1)(r-1),$$

$$a^{\varphi(m)} = a^{(p-1)(q-1)(r-1)}$$

である。まず、 $a = sp \quad (1 \le s < qr)$の場合を考えると、

$$(sp)^{\varphi(m)} = s^{(p-1)(q-1)(r-1)}p^{(p-1)(q-1)(r-1)}$$

$$(sp)^{\varphi(m)} \equiv \begin{cases} 0 & (\mathrm{mod}\, p) \\ \\ 3\text{ 通り} & (\mathrm{mod}\, qr) \end{cases}$$

$$s^{\varphi(qr)} \equiv \begin{cases} 1, \quad 1, \quad 0 & (\mathrm{mod}\, q) \\ \\ 1, \quad 0, \quad 1 & (\mathrm{mod}\, r) \end{cases}$$

$\varphi(qr)$ に $p-1$ を掛けたものを $\varphi(m)$ とおくと

$$s^{\varphi(m)} \equiv \begin{cases} 1, \quad 1, \quad 0 & (\mathrm{mod}\, q) \\ \\ 1, \quad 0, \quad 1 & (\mathrm{mod}\, r) \end{cases}$$

以降は、$a = tq \quad (1 \le t < rp)$, $a = ur \quad (1 \le u < pq)$ とおき、同様な手順を追っていくと、

p	0	1	0	0	1	0	1	1
q	0	0	1	0	1	1	0	1
r	0	0	0	1	0	1	1	1

よって、$\gcd(a, m) \neq 1$, $m = pqr$ のとき $a^{\varphi(m)}$ は、6 種類の整数である。ゆえに、$\gcd(m, a) = 1$ の時と $a \equiv 0\ (\mathrm{mod}\, m)$ の時を含めると、$a^{\varphi(m)}$ は $8 = 2^3$ 種類となる。■

これらの実験や予備的な考察により、次の定理を得た。この定理が本論文の主定理である。

定理 4

m が相異なる n 個の素数の積ならば $a^{\varphi(m)}$ は法 m で 2^n 種類現れる。

証明　$m = p_1\, p_2 \ldots p_n$ のときを考える。($p_1, \ldots, p_n$ は相異なる素数)

mのオイラー関数は

$$\varphi(m) = (p_1 - 1)(p_2 - 1) \ldots (p_n - 1)$$

となる。a が p_kの倍数のとき、$a^{\varphi(m)} \equiv 0 \pmod{m}$ となる。また a が p_k の倍数でないときには、$a^{\varphi(m)} \equiv 1 \pmod{m}$ となる。よって、p_1 から p_n までの因数に対して、

$$a^{\varphi(m)} \equiv \begin{cases} 0 & (\mathrm{mod}\ p_k) \\ & (1 \leq k \leq n) \\ 1 & (\mathrm{mod}\ p_k) \end{cases}$$

となる。中国式剰余定理より、この時の解は法 m で考えてただ一つに決まり、その組み合わせは、p_k ごとに 0 と 1 の 2 通りになるから、m が相異なる n 個の素数の積ならば $a^{\varphi(m)}$ は法 m で 2^n 種類現れる。 ■

4 今後の展望

次の 2 つの課題が未解決のまま残っているので、これは将来の課題としたい。

(1) mを素因数分解したとき重複度が 2 以上のとき

$$m = p^{e_1}q^{e_2}r^{e_3} \ldots \qquad (e_1, e_2, e_3 \geq 2)$$

を考える。

(2) また、卒業研究発表会において、増田哲先生による「$a^{\varphi(m)}$の種類だけでなく、具体的な値もわかりますか」という質問と、岩尾慎介先生による「$m = pqr$のとき、実験によると、真ん中の数がちょうど半分ですが、それは一般的ですか」という質問をいただいた。しかしながら、私の研究にはこのような質問に対応できるだけの十分な時間がなかったため、本論文に記すことはできなかった。そのため、これらのことも今後の課題としたい。増田、岩尾両先生に貴重な質問をいただいたことを感謝する。

5 おわりに

この論文は、整数のべき乗についての研究を行った私の軌跡である。本研究を行った動機としては、この 4 年次の夏休み期間前に整数の性質に興味を持ったからである。そこで夏休みの間に整数論についての文献を読んでいると、ある一つの定理が目に飛び込んできた。これこそが、本研究の一番基礎となっている「フェルマーの小定理」である。その言葉を目にしたところ、私は苦い思いに苛まれることとなった。思い返してみると、私とフェルマーの出会いは古いものとなる。当時中学生であった中川少年は巷で流行っていた漫画本の中に「フェルマーの最終定理」というものを見つけた。そこには、この定理を証明するまでに 360 年という長い年月がかかった。この文章を読み、行きつけのブックオフで驚愕した自分がそこにいた。360 年も解くことができなかった問題がこの世に存在していたのか。これこそが、フェルマーとの出会いであった。しかし、ここまでは全く持って苦い思い出ではない、苦いのはもう少し先の話である。

月日は流れ、少年から青年に変わった私は大学受験生となっていた。町の木々はすっかり葉を落とし、センター試験まであと１か月というところであった。そんな私はというと、今は高校最後の定期試験を受けていた。この数学の試験が終わればもうこの学校で定期試験を受けることは無いのだと思うと何となく名残惜しくもなっていたが、そんな折、私は大問４に挑もうとしていた。のちに聞くところ、この問題はどこかの入試問題の過去問をそのまま出題したものであった。その問題こそが、今回の研究のきっかけとなった「フェルマーの小定理」である。整数の問題が苦手だった当時の私にとって、問題文を読んでもほとんど理解することができず、誘導に沿って解いてみるものの、私の頭の中はちんぷんかんぷんになるだけであった。結局この大問をごっそり落とした私は、他の問題も満足に解けず、帰ってきた答案は赤点ラインを１点越えただけの不本意な点数となっていた。こうして私の高校数学は幕を閉じたのであった。その後の私はというと、何とか大学に合格し紆余曲折しながらも無事に進級でき卒業研究に打ち込むことができている。

私とフェルマーという、この何とも不思議な巡り合わせは、実は奇跡であるといえるのではないか感じている。大学生活の最後で研究できてとてもよかった。この感謝の気持ちを西山教授に贈りたい。ありがとうございました。

中川　貴仁

6 参考文献

[1] 小林昭七、「なっとくするオイラーとフェルマー」 （講談社、2003 ）

[2] 雪江明彦、「初等整数論から p 進数へ」 （日本評論社、2013）